

**Appln No. 09/690,243**  
**Amdt date August 20, 2008**  
**Reply to Office action of May 20, 2008**

**REMARKS/ARGUMENTS**

Claims 1-4, 8, 10-40, and 42-79 are pending. Claims 1, 32-39, 42, 44, 47, 60, and 73-79 are amended.

Dependent claims 32 and 72 are allowed. Claims 32 and 72 are now rewritten in an independent form, therefore, allowance of these claims and dependent claims 33-38 and 73-79, which now depend on the allowed rewritten independent claims 32 and 72 is respectfully requested.

Claims 1-4, 8, 10-31, 33-40, 42-71 and 73-79 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Whitehouse (US 6,005,945) in view of Pang (US 6,446,204).

Amended independent claim 1 includes, among other limitations, "a plurality of stateless cryptographic devices remote from the client system and capable of authenticating and processing VBI printing requests from any of the plurality of users," and "wherein when a VBI printing request from a current user is received by the server system, an available cryptographic device . . . and the database cross-verify a copy of a last transaction data record stored in the database and stored in the available cryptographic device, before processing the VBI printing request from the current user." Applicant respectfully submits that the combination of Whitehouse and Pang does not teach or suggest the above limitations.

**First**, regarding the limitation of "an available cryptographic device . . . and the database cross-verify a copy of a last transaction data record stored in the database and stored in the available cryptographic device, before processing the VBI printing request from the current user," there is no teaching or suggestion in Whitehouse for this limitation.

Applicant respectfully disagrees with the Examiner's assertion (with respect to claim 13) that Whitehouse in col. 8, line 63 to col. 9, line 12 teaches "wherein the database stores a first set of one or more last database transactions and each cryptographic device stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction," as recited by claim 13. The cited text of Whitehouse simply discloses that "when verifying the postage indicia

**Appln No. 09/690,243**  
**Amdt date August 20, 2008**  
**Reply to Office action of May 20, 2008**

on mail pieces" [that is after the postage has been printed on an envelop and mailed] . . . if the serial number on a mail piece is sufficiently different from the serial numbers on other mail pieces recently processed for the same meter, the postal service computer may request a copy of the meter's recent postage purchase history to determine if the postal indicia on the mail piece being processed is authentic," That is to determine if "a mail piece is . . . fraudulent." (Col. 8, line 67 to col. 9, line 8, emphasis added.). This is clearly different from "an available cryptographic device . . . and the database cross-verify a copy of a last transaction data record stored in the database and stored in the available cryptographic device, before processing the VBI printing request from the current user," and "wherein the server system sends a print authorization to the client system to print a VBI when the copy of the last transaction data record is cross-verified," as recited by the amended claim 1. Similarly Pang, alone or in combination with Whitehouse, does not teach or suggest the above limitation.

Second, with regard to the limitation of "a plurality of cryptographic devices remote from the client system," Whitehouse does not have any cryptographic devices remote from the client system. Nevertheless, the Examiner construes the central computer(s) 102 as the "plurality of cryptographic devices remote from the client system." However, neither these central computers 102, nor their Encryption Procedures (software) 162 stored in the local memory 154 of the central computer 102 can be construed as "cryptographic devices." (Col. 8, lines 38-40 and FIG. 4, underlining added.). Also, see, col. 9, line 19: "encryption software and keys." Pang does not have any cryptographic devices either.

The specification is clear about the definition of a "cryptographic device." For example, on page 20, lines 21 to 26, the specification emphasizes that "[i]n one embodiment of the present invention, the cryptographic modules 52 are FIPS 140-1 certified hardware cards that include firmware to implement PSD functionality in a cryptographically secure way. The cryptographic modules are inserted into any of the servers in the Postal Server Infrastructure." (Underlining added for emphasis). Additionally, "each cryptographic module is a stateless device, meaning that a PSD package can be passed to any device." (Page 8, lines 16-17, underlining added.).

Accordingly, neither the central computers 102 of Whitehouse, nor their Encryption Procedures (software) 162 stored in the local memory 154 can be construed as "cryptographic devices." Likewise, Pang, alone or in combination with Whitehouse, does not teach or suggest the above limitation.

Third, with respect to the limitation of "a plurality of cryptographic devices . . . capable of authenticating and processing VBI printing requests from any of the plurality of users," there is no teaching or suggestion in Whitehouse for this limitation either. Rather, Whitehouse's central computers 102 are not capable of "authenticating and processing VBI printing requests from any of the plurality of users," because each central computer 102 of Whitehouse (even assuming there are more than one) stores the Customer Database 172 and the Transaction Database 174 in its own local memory (RAM) 154 and the transaction database 174 stores records concerning each postage indicium generated by the secure central computer 102. (Col. 8, lines 54-62 and FIG. 4, underlining added.). Therefore, one skilled in the art of computer architecture would readily realize that with this Whitehouse's system architecture, the central computers 102 cannot process any of the plurality of users," **because the central computers do not have access to all users' information, some of which is stored in the local memories of the other central computers**. For the same reasoning, in Whitehouse's central computers 102 environment, in which Customer Database 172 and the Transaction Database 174 are stored in each computer's own local memory (RAM) 154, a user can NOT be authenticated using any of the cryptographic devices (even assuming that a central computer with "encryption software" can be construed as a cryptographic device).

Moreover, Pang, alone or in combination with Whitehouse, does not teach or suggest "processing VBI printing requests from any of the plurality of users."

In short, based on at least the above-mentioned three arguments, each of which deemed sufficient by itself, the amended independent claim 1 is patentable over cited references.

Amended independent claim 39 includes, among other limitations, "cross-verifying a copy of last transaction data record stored in the database and stored in an available cryptographic device, before processing the VBI printing request from the user," and

**Appln No. 09/690,243**  
**Amdt date August 20, 2008**  
**Reply to Office action of May 20, 2008**

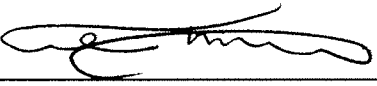
"authenticating the user by the cryptographic device in a stateless manner utilizing a respective one-of the plurality of transaction data record stored in the database." As discussed above, the combination of Whitehouse and Pang does not teach or suggest the above limitations. Consequently, claim 39 is also patentable over cited references.

In short, independent claims 1 and 39 are patentable in view of the cited references. The remaining dependent claims 2-4, 8, 10-31 and 42-47 and 49-71 depend from claims 1 and 39, respectively and include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested.

Applicant respectfully encourages the Examiner to contact the undersigned at (626) 795-9900 if there are any questions.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By   
Raymond R. Tabandeh  
Reg. No. 43,945  
626/795-9900

RRT/clv

CLV PAS808748.1-\*08/20/08 3:08 PM